

FIELD OF THE INVENTION

11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044

10

15

20

As the world becomes more and more reliant on digital communications and systems, it is expected that mobile phones and PDA's will become more and more useful. For example, the use of personal identification number (PIN) codes are becoming more and more common for verifying the identity of a user of a digital system such as, for example, a bank automatic teller machine (ATM). As more and more digital systems adopt the use of PIN codes for identity verification, the number of PIN codes that a user of these digital systems must remember increases, particularly since it is often recommended for security purposes that users use different PIN codes for different digital systems. As a result of this increase in the number of PIN codes that must be remembered, some users of mobile phones and PDA's have begun to store their PIN codes in digital read/write memory which is now incorporated within most of these devices. That is, some users of mobile phones and PDA's have begun storing their PIN codes in the digital read/write memory that is now incorporated within their mobile phones and PDA's, rather than trying to memorize all of the increasing number of PIN codes that must be used to gain access to a corresponding increasing number of digital systems.

Despite the apparent benefit of storing PIN codes in the digital read/write memory of mobile phones or PDA's, a security problem exists with this practice. That is, the digital read/write memory in existing mobile phones and PDA's is not capable of preventing unauthorized users from accessing PIN codes stored therein. The only way that PIN codes, or any other data, that are stored within the digital read/write memory of a mobile phone or PDA are truly secure is if the digital read/write memory can withstand four basic types of attack. Namely, these four basic types of attack include: 1.) when an attacker *cannot read* the content of the memory and *does not know* (before the attack) anything that has been stored in the memory; 2.) when an attacker *can read* the content of the memory but *does not know* (before the attack) anything that has been stored in the memory; 3.) when an attacker *cannot read* the content of the memory but *does know* (before the attack) at least one thing that has been stored in the memory; and 4.) when an attacker *can read* the content of the memory and *does know* at least one thing that has been stored in the memory. Thus, for PIN codes, or any other data, that are stored within the digital read/write memory of a mobile phone or PDA to be truly safe and secure, the memory

has to be resistant to all the different types of attacks listed above.

In view of the foregoing, it would be desirable to provide a technique for securely storing data within a memory which overcomes the above-described inadequacies and shortcomings while also withstanding all of the above-described types of attacks.

OBJECTS OF THE INVENTION

The primary object of the present invention is to provide a technique for securely storing data within a memory in an efficient and cost effective manner.

The above-stated primary object, as well as other objects, features, and advantages, of the present invention will become readily apparent to those of ordinary skill in the art from the following summary and detailed descriptions, as well as the appended drawings. While the present invention is described below with reference to preferred embodiment(s), it should be understood that the present invention is not limited thereto. Those of ordinary skill in the art having access to the teachings herein will recognize additional implementations, modifications, and embodiments, as well as

other fields of use, which are within the scope of the present invention as disclosed and claimed herein, and with respect to which the present invention could be of significant utility.

SUMMARY OF THE INVENTION

5 According to the present invention, a technique for securely storing data within a memory is provided. In a preferred embodiment, the technique is realized by encrypting the data (e.g., one or more PIN codes) using a non-verifiable personal identifier, and then encrypting a reminder (e.g.,
10 some user-identifiable code) using the same non-verifiable personal identifier. The encrypted data and the encrypted reminder are then stored in the memory. The stored encrypted data and the stored encrypted reminder can only be correctly decrypted using the non-verifiable personal identifier. Also,
15 a correctly decrypted reminder provides an indication of correctly decrypted data.

 In accordance with other aspects of the present invention, the non-verifiable personal identifier is not stored in the memory. Examples of the non-verifiable personal
20 identifier include alphanumeric characters and identifiable

personal characteristic such as, for example, a human voice,
a human fingerprint, and a human eye.

In accordance with further aspects of the present
invention, the non-verifiable personal identifier is applied
5 against the stored encrypted data and the stored encrypted
reminder so as to decrypt the stored encrypted data and the
stored encrypted reminder. The original data may then be
provided to a user after being correctly decrypted using the
using the non-verifiable personal identifier. For example,
10 the original data may be displayed to a user or the original
data may be announced to a user. Similarly, the original
reminder may be provided to a user after being correctly
decrypted using the using the non-verifiable personal
identifier. For example, the original reminder may be
15 displayed to a user or the original reminder may be announced
to a user. A predetermined time period is beneficially
required before applying another personal identifier against
the stored encrypted data and the stored encrypted reminder
for the purpose of decrypting the stored encrypted data and
20 the stored encrypted reminder.

In accordance with still further aspects of the present
invention, an identifier other than the non-verifiable

personal identifier may be applied against the stored encrypted data and the stored encrypted reminder so as to incorrectly decrypt the stored encrypted data and the stored encrypted reminder. If such is the case, incorrect data may then be provided to a user after the encrypted data has been incorrectly decrypted using an identifier other than the non-verifiable personal identifier. For example, the incorrect data may be displayed to a user or the incorrect data may be announced to a user. Similarly, an incorrect reminder may be provided to a user after the encrypted reminder has been incorrectly decrypted using an identifier other than the non-verifiable personal identifier. For example, the incorrect reminder may be displayed to a user or the incorrect reminder may be announced to a user. A predetermined time period is again beneficially required before applying another personal identifier against the stored encrypted data and the stored encrypted reminder for the purpose of decrypting the stored encrypted data and the stored encrypted reminder.

The present invention will now be described in more detail with reference to exemplary embodiments thereof as shown in the appended drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

In order to facilitate a fuller understanding of the present invention, reference is now made to the appended drawings. These drawings should not be construed as limiting the present invention, but are intended to be exemplary only.

Figure 1 is a schematic diagram of a system for securely storing data in a memory in accordance with the present invention.

Figure 2 is an illustration of a code bank within a memory of the system shown in Figure 1.

Figure 3 is a flowchart detailing the method used to decrypt one or more encrypted PIN codes and an encrypted reminder code in accordance with the present invention.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENT(S)

Referring to Figure 1, there is shown a system 10 for securely storing data in a memory in accordance with the present invention. The system 10 comprises a processor 12, a memory 14, a plurality of input devices 16, and a plurality of output devices 18. The plurality of input devices 16 comprise a keyboard/touchpad 20, a fingerprint sensor 22, a microphone 24, a retina scanner 26, and a variety of other input devices

which are commonly known in the art. At least one of the plurality of input devices 16 is required in the system 10, although more than one of the plurality of input devices 16 may also be present. The plurality of output devices 18
5 comprise a visual display 30 (e.g., a liquid crystal display), a speaker 32, and a variety of other output devices which are commonly known in the art. At least one of the plurality of output devices 18 is required in the system 10, although more than one of the plurality of output devices 18 may also be
10 present. The system 10 is preferably implemented within a mobile phone or personal digital assistant (PDA), although the present invention is not limited in this regard.

The system 10 operates to a large extent by processing input data provided by the one or more input devices 16 and
15 generating output data for the one or more output devices 18. The processor 12 processes the input data and generates the output data based upon instructions in software program(s) that are stored in the memory 14. The memory 14 also stores encrypted data such as, for example, encrypted personal
20 identification number (PIN) codes, that is to be securely stored in accordance with the present invention.

In the exemplary case of securely storing one or more PIN codes, a user of the system 10 enters the one or more PIN codes and a reminder code through one of the plurality of input devices 16. For example, the user may type/punch a PIN code and a reminder code into the keyboard/touchpad 20. Alternatively, the user may recite a PIN code and a reminder code into the microphone 24. Alternatively still, the user may enter the one or more PIN codes and the reminder code through different means (e.g., a PIN code may be entered through the keyboard/touchpad 20, while the reminder code may be entered through the microphone 24). In any case, the processor 12 receives the one or more PIN codes and the reminder code from one or more of the plurality of input devices 16.

Either before or after the one or more PIN code and the reminder code have been entered, the user of the system 10 must also enter a personal identifier through one of the plurality of input devices 16. The personal identifier can take one of many different forms. For example, the personal identifier may be a compilation of alphanumeric characters that are typed/punched into the keyboard/touchpad 20. Alternatively, the personal identifier may be a compilation of

alphanumeric characters or a term, phrase, or sound that is spoken or otherwise entered through the microphone 24. Alternatively still, the personal identifier may be a fingerprint of the user that is entered through the fingerprint sensor 22. Alternatively even still, the personal identifier may be an eye of the user that is entered through the retina scanner 26. Of course, the present invention is not limited to the above-described examples of personal identifiers. However, whatever form the personal identifier takes, it is received by the processor 12 from one or more of the plurality of input devices 16.

Once the processor 12 receives the one or more PIN codes, the reminder code, and the personal identifier from one or more of the plurality of input devices 16, the processor 12 encrypts the one or more PIN codes and the reminder code using the personal identifier. That is, the processor 12 uses the personal identifier to encrypt the one or more PIN codes and the reminder code. The processor 12 then stores the one or more encrypted PIN codes and the encrypted reminder code in the memory 14. The portion of the memory 14 that stores the one or more encrypted PIN codes and the encrypted reminder code may be referred to as a code bank 40, as shown in Figure

2. That is, the code bank 40 includes the one or more encrypted PIN codes 42 and the encrypted reminder code 44.

At this point it should be noted that the personal identifier is not stored in the memory 14 or by the processor

5 12. That is, after the processor 12 uses the personal identifier to encrypt the one or more PIN codes and the reminder code, the processor then deletes the personal identifier from the memory 14 (if the processor 12 temporarily stores the personal identifier within the memory 14) or from
10 the processor 12 itself. Thus, the key for encrypting the one or more PIN codes and the reminder code (i.e., the personal identifier) is not stored within the system 10. This is an important feature of the present invention, as it insures that the system 10 is resistant to the various forms of attack
15 listed above.

When the user of the system 10 wants to retrieve the one or more encrypted PIN codes from the memory 14, the personal identifier is required to decrypt the one or more encrypted PIN codes and the encrypted reminder code. That is, just as
20 the user of the system 10 had to enter the personal identifier to encrypt the one or more PIN codes and the reminder code, the user of the system 10 also has to enter the personal

identifier to decrypt the one or more encrypted PIN codes and the encrypted reminder code. Thus, the user of the system 10 enters the personal identifier through one of the plurality of input devices 16, and the processor 12 then uses the personal
5 identifier to decrypt the one or more encrypted PIN codes and the encrypted reminder code. The one or more decrypted PIN codes and the decrypted reminder code are provided to the user through one of the plurality of output devices 18. For example, the one or more decrypted PIN codes and the decrypted
10 reminder code may be provided to the user through the visual display 30 (e.g., a liquid crystal display) or through the speaker 32. Of course, the present invention is not limited to the above-described examples of output devices.

The decrypted reminder code acts as an indication to the
15 user of system 10 that the one or more decrypted PIN codes are in fact a reproduction of the original pre-encrypted PIN codes. That is, if the user of the system 10 recognizes the decrypted reminder code as the pre-encrypted reminder code, then the user of the system 10 can be confident that the one
20 or more decrypted PIN codes are in fact a reproduction of the original pre-encrypted PIN codes. On the other hand, if the user of the system 10 does not recognize the decrypted

reminder code as the pre-encrypted reminder code, then the user of the system 10 understands that the one or more decrypted PIN codes are not a reproduction of the original pre-encrypted PIN codes. That is, if an incorrect personal identifier is entered when trying to decrypt the one or more encrypted PIN codes and the encrypted reminder code, then the processor 12 will decrypt the one or more encrypted PIN codes and the encrypted reminder code based upon this incorrect personal identifier and the one or more decrypted PIN codes and the decrypted reminder code that are subsequently provided to the user of the system 10 will not be a reproduction of the original pre-encrypted PIN codes and the original pre-encrypted reminder code. This is an important feature of the present invention, as it only allows the true user of the system 10 to know whether the one or more decrypted PIN codes are in fact reproductions of the original pre-encrypted PIN codes since only the true user of the system 10 should know the original pre-encrypted reminder code. Thus, this important feature of the present invention also insures that the system 10 is resistant to the various forms of attack listed above.

Another important feature of the present invention that may further insure that the system 10 is resistant to the various forms of attack listed above is the inclusion of a timer program that may be stored in the memory 14 and run by the processor 12. For example, after every attempt to enter a personal identifier, the processor 12 may prevent another attempt for a predetermined period of time (e.g., 10 minutes). This would only allow an attacker 6 attempts per hour to try to crack the system 10. Referring to Figure 3, there is shown a flowchart 50 detailing the method used to decrypt the one or more encrypted PIN codes and the encrypted reminder code, which incorporates this further important feature in accordance with the present invention.

To summarize the forgoing, by encrypting the PIN codes with a personal identifier, the system 10 is resistant to attacks 2 and 4 as described above. Also, by not storing the personal identifier in the system 10 (for verification purposes or otherwise), the system 10 is resistant to attacks 1 and 2 as described above. Further, by requiring that a subsequent personal identifier be entered only after a predetermined time period has elapsed, the system 10 is resistant to attack 3 as described above.

The present invention is not to be limited in scope by the specific embodiments described herein. Indeed, various modifications of the present invention, in addition to those described herein, will be apparent to those of ordinary skill in the art from the foregoing description and accompanying drawings. Thus, such modifications are intended to fall within the scope of the following appended claims. Further, although the present invention has been described herein in the context of a particular implementation in a particular environment for a particular purpose, those of ordinary skill in the art will recognize that its usefulness is not limited thereto and that the present invention can be beneficially implemented in any number of environments for any number of purposes. Accordingly, the claims set forth below should be construed in view of the full breath and spirit of the present invention as disclosed herein.